TEMPLATE: BUSINESS ASSOCIATE AGREEMENT

Introduction

The Business Associate Agreement Template should be added to any contract or memorandum of understanding when Protected Health Information (PHI) is being transferred to an organization or person providing a service for the organization originating the PHI. This template, with appendices, fulfills HIPAA requirements to safeguard the confidentiality of PHI.

Purpose

The purpose of this template is to ensure that HIPAA confidentiality requirements for PHI are met when PHI is transferred to a Business Associate and employees and contractors of Business Associates.

Reference:

45 CFR Subtitle A, Subchapter C, Part 160, Subpart A (160.103 Definitions)
45 CFR, Subtitle A, subchapter C, Part 164, Subpart E in general; in particular 164.502(e)(1), (e)(2) (this template required by (e)(2))
45 CFR, Subtitle A, subchapter C, Part 164, 164.504 (e)(1), (e)(2), (e)(3) and (e)(4)
45 CFR, Subtitle A, subchapter C, Part 164, 164.512 (I)
45 CFR, Subtitle A, subchapter C, Part 164, 164.514

Assumptions:

Those individual records containing PHI are provided

Pre-Requisites:

Standard business operating procedures for state agencies as required by the State Administrative Manual and applicable statutes and regulations pertaining to contract law and practices.

Pertains to organizations contracting with another organization that provides a service, the purpose for which Protected Health Information is provided.

Created: February, 2001 Contact:
Revised: Phone:
E-Mail:

Constraints:

See Penalties

Dependencies:

Standard business operating procedures for State Agencies as required by the State Administrative Manual and applicable statutes and regulations pertaining to contracts and agreements.

Procedures:

Preventive Measures:

- Ensure review by Legal staff within impacted organizations
- Ensure the Business Associate Agreement, and its provisions, are incorporated into each contract, memorandum of understanding, etc., pertaining to the transmission of PHI as described in the HIPAA Privacy Rules.

Guidelines:

- Risk points exist whenever there is interface between organizations in the transfer of data. This Agreement should be used to address each area of risk.
- Use whenever transferring PHI to another organization performing a service.
- The attached Template contains five parts:
    1. **Business Associate Agreement**: use whenever transfering PHI to another organization performing a service;

    2. **Appendix A Plan for Maintaining Confidentiality and Security of Data:** The purpose of these requirements is to provide a framework for maintaining confidentiality and security of data compiled for the (entity) or its subcontractors;

    3. **Appendix B Contract Employee Confidentiality agreement:** Ensures that employees of contractors and subcontractors are aware of and enforce required privacy provisions of the agreement.

    4. **Glossary of Terms**

    5. **Workgroup Participants**

Monitoring Compliance Criteria:

- Organizations should ensure a process exists to obtain, monitor, and respond to complaints from both internal and external sources.

- It is recommended that the Agency Privacy Officer group be established and enabled to promulgate modifications to the standard Business Associate agreements as required.

Enforcement:

- Roles and Responsibilities for the Department/Agency Privacy Officers should incorporate monitoring and enforcement of these provisions.

- Covered Entities and their Associates should cooperate in resulting assessments and/or investigations.

- Health and Human Services (HHS) Office of Civil Rights (OCR) maintains discretionary enforcement based on:
  Harm done
  Willingness to achieve compliance
  Delay enforcement to permit compliance where violations due to reasonable cause

Penalties for Non-Compliance:

Statutory Penalties Include:

- Financial penalties for failure to comply
  $100 per violation/person, not to exceed $25,000 annually

- Criminal penalties for knowingly disclosing or obtaining PHI or using a unique health identifier without permission:

Knowingly	$50,000 and/or 1year
False pretenses	$100,000 and/or 5years
Use for commercial or Personal gain or Malicious harm	$250,000 and/or 10 years

Business Associate Agreement

Introduction

THIS BUSINESS ASSOCIATE AGREEMENT Addendum is made as of [date] by and between [Contracting Entity] entity, with offices at [address] and [Name of business associate] business associate, a [corporation, company or Department] with offices at [address].

[Entity] and [Partner] have entered into this Business Associate Agreement to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the (draft) Security and Electronic Signature Rule, and the Final Privacy regulation requirements for such an Agreement, as well as our duty to protect the confidentiality and integrity of protected health information as required by law, Department policy, professional ethics, and accreditation requirements. Parties signing this Agreement shall fully comply with the provisions of the Regulations implementing HIPAA.

[Entity] and [Partner] desire to facilitate the [provision of][billing or transfer of protected health information] by electronically transmitting and receiving data in agreed formats and to assure that such transactions comply with relevant laws and regulations.

NOW THEREFORE, the parties, intending to be legally bound, agree as follows:

Section 1. Prerequisites.

1.1. Document Standards. Each party may transmit to, or receive from, the other party, either electronically or using other media, protected health information (Individually Identifiable Health Information) as specified by written agreement as part of Appendix __.[1] All documents shall be transmitted in accordance with the standards set forth in Appendix __.[2]

1.2.1. Third Party Service Providers. The parties will transmit Documents electronically to each party either, as specified in the Appendix, directly or through any third party service provider with which either party may contract. Either party may modify its election to use, not use, or change a third party service provider upon __ days prior written notice. Selection of a third party service provider and any subsequent contractors must be approved by [Entity]. Contracts with a third-party service provider must be approved by [Entity].

1.2.2. Costs of Third Party Service Providers. Each party shall be responsible for the costs of any third party service provider with which it contracts unless otherwise set forth in the Appendix.

[1] Statement ofWork, or equivalent.
[2] Security requirements as specified in Appendix __.

1.2.3. Liability for Acts of Third Party Service Providers. Each party shall be liable for the acts or omissions of its third party service provider while transmitting, receiving, storing, or handling Documents, or performing related activities, for, with, to, or from such party; provided that if both the parties use the same third party service provider to effect the transmission and receipt of a Document, the originating party shall be liable for the acts or omissions of such third party service provider as to such Document. All subsequent contractors shall abide by the provisions of this Agreement, and these provisions must be included in the contract.

1.3. System Operations. Each party, at its own expense, shall provide and maintain the equipment, software, services, and testing necessary to effectively, reliably, and confidentially transmit and receive Documents.

1.4. Security Procedures. Each party shall properly use those security procedures, including those specified in the Appendix, which are reasonably sufficient (a) to ensure that all transmissions of Documents are authorized, (2) to protect the integrity and confidentiality of protected health information, and (3) to protect its business records and data from improper access.

1.5. Signatures. Each party shall adopt as its signature (ASignature@) an electronic identification known as "digital signature" to be verified by transmitting a digital certificate.[3] Private keys used in digital signatures may not be disclosed to other than the party that owns the private key.The digital signature and certificate shall be affixed to or contained in each Document transmitted by such party. Each party agrees that any Signature of such party affixed to or contained in any transmitted Document shall be sufficient to verify that such party originated such Document. Neither party shall disclose to any unauthorized person the Signature of the other party.

Section 2. Transmissions.

2.1. Proper Receipt. Documents shall not be deemed to have been properly received, and no Document shall give rise to any obligation, until decrypted and accessible to the receiving party at such party's Receipt Counter designated in the Appendix.

2.2. Verification. Upon proper receipt of any Document, the receiving party shall promptly and properly transmit a functional acknowledgment in return, unless otherwise specified in the Appendix. A functional acknowledgment shall constitute conclusive evidence that the receiving party has properly received a Document

Section 3. Integrity and Confidentiality of Medical Information.

[3] This is the recommended Agency-wide standard, although it is not specifically required by HIPAA.

3.1. Integrity. The parties will take reasonable measures to protect the integrity of all Documents and data. Neither party will insert any virus, key locks, or other programs into the system, regardless of whether or not a dispute exists between the parties. If the contract is for a defined period of time, the receiving party will return the information in usable form upon request or at the end of the contract, and shall [secure]destroy any copies or extracts of the protected health information in its possession. .

3.2. Confidentiality. The parties will keep all protected health information concerning identifiable patients strictly confidential and use such information only for the purposes of providing services under the contract. The parties will disclose such information only to those of their employees who have authorized access to the information, who have received privacy training, and who have signed an agreement to hold the information in confidence. Neither party will redisclose such information except with the subject individuals express consent or as otherwise authorized by law. Each party agrees to disclose only the minimum necessary information for each access to protected data. Each party agrees not to re-identify de-identified information, except that the covered entity originating the information may re-identify de-identified information using a key that itself contains no information. Partner agrees that it will not seek to release information through a Privacy Board or Institutional Review Board (IRB) without prior written consent of Entity

3.3. Indemnification. A breaching party agrees to indemnify the other for any special, incidental, exemplary, or consequential damages, including legal fees and costs, if the other party is found liable for or otherwise hardened by a breach of integrity or confidentiality that Is the fault of the breaching party.

Section 4. Miscellaneous.

4.1. Termination. This Agreement shall remain in effect unless terminated for cause by [Entity] with immediate effect, or until terminated by either party with not less than __ days prior written notice to the other party, which notice shall specify the effective date of the termination; provided, however, that any termination shall not affect the respective obligations or rights of the parties arising under any Documents or otherwise under this Agreement before the effective date of termination. Upon termination, [Partner] shall destroy any copies or extracts of the protected health information in its possession and shall certify to Entity that such destruction has occured.. .

4.2. Severability. Any provision of this Agreement that a court of competent jurisdiction determines to be unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of this Agreement.

4.3. Force Majeure. No party shall be liable for any failure to perform its obligations in connection with any Transaction or any Document where such failure results from any act of God or other cause beyond such party's reasonable contro1 (including, without limitation, any mechanical, electronic, or communications failure) that prevents such party from transmitting or receiving any Documents.

4.4. Limitation of Damages. Other than as specified in paragraph 3.3, neither party shall be liable to the other for any special, incidental, exemplary, or consequential damages arising from or as a result of any delay, omission, or error in the electronic transmission or receipt of any Documents pursuant to this Agreement, even if either party has been advised of the possibility of such damages.

4.5. Adjudication. Any controversy or claim arising out of or relating to this Agreement or the breach thereof, shall be settled in accordance with the laws of the State of California.

EACH PARTY has caused this Agreement to be properly executed on its behalf as of the date first above written.

For: [Name of Entity]	For: [Name of Partner]
BY: _____	BY:
_____	
[printed name & title – Director or Designee]	[printed name & title - CEO, Director or Designee]
Division Chief/Deputy Director Program Manager (Branch Chief & Above) Information Security Officer (ISO) Privacy Officer	Security Officer Privacy Officer

APPENDIX A

PLAN FOR MAINTAINING CONFIDENTIALITY AND SECURITY OF (ENTITY) DATA

I. GENERAL REQUIREMENTS

The purpose of these requirements is to provide a framework for maintaining confidentiality and security of data compiled for the (entity) or its subcontractors. These data are the property of the (entity). While the requirements in this document set forth the Plan for Maintaining Confidentiality and Security of Data, it does not replace the requirements and responsibilities as sited in the Contract/MOU. Therefore, the information and stated requirements as set forth in the Business Associate Agreement are hereby incorporated by reference.

II. DATA SECURITY

A. Redisclosure of the source, (Entity) Confidential data

1. All contractors seeking access to confidential (entity) data files must request access from the (entity). Under no circumstances is the contractor to redisclose nor re-release source confidential (entity) data.

2. Any persons not affiliated with the contractor nor included under this Contract/MOU with the (entity) are to be referred to the (entity) to formally request access to the confidential data.

B. Data Security Requirements

1. All contractors and their subcontractors are responsible for security of the (entity) data.

2 All contractors and their subcontractors must ensure that electronic media that contains confidential or sensitive data is protected at the level of the most confidential or sensitive piece of data on the media.

3. All contractors and their subcontractors must comply with the Guidelines for Protection of Confidential and Sensitive Data, as follows:

- Confirm the identity of any individual who has requested confidential or sensitive data.
- When there is a business need to discuss confidential (entity) information within the office, discuss the information in an enclosed room, if possible.
- Log off from all networked systems that contain confidential or sensitive (entity) information whenever you leave your work area for an extended period of time.
- Take precautions to ensure that each fax containing confidential and sensitive (entity) materials were appropriately received.

4. Data Transmission

   a. Adequate steps must be taken to ensure the confidentiality of data transmission. Data transmitted over public networks must be encrypted using non-proprietary, secure, generally available encryption software.

   b. There are various methods to transfer confidential data between the (entity), contractors and subcontractors. These confidential data contain sensitive and confidential information including name, address, social security number, and administrative case number, etc. The various methods for transfer of data include transfer on tape/cartridges or File Transfer Protocol (FTP). The information that follows will describe these methods of data transfer and preferred standards to ensure confidentiality of the data.

   c. Data transferred via tape or cartridge

      The (entity) requires that confidential data transferred on cartridges or tapes be encrypted. Additionally, the tapes and cartridges are delivered via a secure mail service, such as Federal Express or registered U.S. Mail.

   d. Data transferred electronically

      The (entity) requires that all FTP accounts that transfer confidential data with personal identifiers be highly restricted. These accounts must maintain an audit trail. These accounts are to be accessible to a limited number of contractor and/or subcontractor staff. No other accounts on contractor and/or

subcontractor's computers can have access to this account. The contractor and/or subcontractor or is to maintain a current listing of the personnel who have access to the FTP account.

Additionally, all confidential data transferred from contractor and/or subcontractor machines are to be encrypted; there are no exceptions.

e. Data transferred via paper copy

The (entity) requires that paper copies of confidential data be mailed via a secure mail, such as Federal Express or registered U.S. Mail.

Additionally, the (entity) requires that paper copies of confidential data are stored in a locked file cabinet. Access to the key is to be highly restricted.

f. Working with intermediate files with confidential identifiers

Confidential identifiers as specified by (entity) are to be replaced with non-confidential identifiers as soon as possible in the processing of the (entity) data.

C. Network Security Requirements

1. The contractor is to provide the following electronic access measures at a minimum:

- Provide a notification at initial logon that law prohibits unauthorized access.

- Provide an audit trail. This audit trail shall identify all accesses to the source file, success or failure of the access, the completion status of the access (e.g. "failed authentication", "successful", "user terminated") and the record and field modified.

- Provide a method for verification of the individual accessing the system. (Refer to Section 1.4 through 1.5 of Agreement)

- Limit access to data to those authorized employees of the contractor who have a functional requirement to use the data.

- Provide the capability of revoking access from a user after three

unsuccessful access attempts.

- Have a security manual or package, which will adequately protect against loss or unauthorized (accidental or intentional) access, use, disclosure, modification, and destruction of data.

D. Storage of Confidential Data

The (entity) requires that all media containing confidential information is to be stored in a secured area (a locked room or locked file cabinet). Keys to these locks are to be held by a limited number of contractor/subcontractor personnel.

E. Destruction of Confidential Data

The contractor and their subcontractors shall destroy all confidential data an or witnessed destruction. Destruction standards must be in accordance with the National Security Center Standards ("***A Guide to Understanding Data Remanence in Automated Information Systems***").

F. Contractor Staff

1. The contractor is obligated to ensure that confidential data are not accessible to former employees of the contractor.

2. It is the responsibility of the contractor to have a record of the access authorization for each individual employee that has access to the confidential data. The security systems administrator(s) must maintain an appointment/separation checklist for each employee which documents how access authorization was modified when any employee terminates employment or changes duties.

G. Information Security Incidents

1. The contractor shall immediately notify the (entity) or its designated agent of any actual or attempted information security incidents. Information security incidents must be reported by telephone to:

   Name
   (Entity) Information Security Officer
   Organization
   Telephone Pager Cellular Phone

2. A security incident, for purposes of this agreement, includes, but are not limited to, the following: any event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized disclosure of (entity) information assets. These incidents are classified in the following types: (1) viruses, (2) theft of (entity) information assets, (3) misuse of information assets, (4) destruction of information assets, (5) intrusions (electronic and physical), and (6) any other types of information security incident that does not fit into the previous categories.

3. The contractor shall cooperate in any investigations of information security incidents.

H. Confidentiality Statements

1. All staff of the contractor must sign a confidentiality agreement. (Refer to Appendix B)

2. The supervisor of the employee shall review the signed confidentiality agreement with the employee and document this review

I. Security Systems Administrator Duties

1. The contractor shall designate a single person as the security systems administrator. The name of the individual so designated shall be supplied to the (entity).

2. The security systems administrator must have the ability to change or remove any computer access authorization of an individual having access to the system at any time.

3. The contractor must have security clearance procedures used to ascertain if the employee who performs the duties of the security systems administrator is a trusted person who has demonstrated in past jobs a capability to perform in this role. Additionally, these security clearance procedures must ascertain if the employee who performs the duties of security systems administrator has any criminal or past job background, which would call into question their ability to perform this role successfully.

J. Risk Analysis

The contractor must carry out a risk analysis with sufficient regularity, or as specified by (entity), to identify and assess vulnerabilities associated with all information assets owned, maintained or used by the contractor, and define a cost-effective approach to manage such risks. Specific risks that must be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of employees and outsiders; fire, flooding, and electrical disturbances; and loss of data communications capabilities. The contractor shall advise the (entity) or its designated agent of any vulnerability that may present a threat to the information and of the specific safeguards for protecting the (entity) information. The contractor shall take the necessary steps to protect the data as a condition of the Contract/MOU.

K. Physical Access/Events

1. Physical security measures must provide for the management control of physical access to information assets (including PC systems and computer terminals), the prevention, detection and suppression of fires, and the prevention, detection, and minimization of water damage.

2. Data shall be stored in a place physically secure from access, use, modification, disclosure, or destruction by an unauthorized person. Information in electronic format, such as magnetic tapes or discs, must be stored and processed in such a way that an unauthorized person cannot retrieve the information by computer, remote terminal or other means.

2. Contingency plans must be established and implemented in order to assure that operations can be back to normal in minimum time after natural or man-made disasters, unintentional accidents, or intentional acts such as sabotage. These plans must include, but are not limited to, the regular backup of automated files and databases, secure storage, and recovery and restarting planning procedures.

L. On-line Access

If the contractor develops any on-line access, this on-line system must have adequate security measures. These measures must include, but are not limited to, the development of passwords and access controls to protect the security of the data from any individual who is not authorized to access with the data.

M. Rules of Aggregation ***(For Research Projects: Modification may be required by the user to ensure meet requirements of the*** **organization)**

The contractor shall not disclose any individually identifiable information. The contractor shall ensure that the data are aggregated to geographic regions larger than 100,000 persons in the sample area are.

N. Rules and Guidelines of Aggregation

1. Principle--The guiding principle of the rules of aggregation of data for the purposes of the (entity) confidential data is that no one will be able to discern an individual participant. The contractor shall interpret this principle to override the suggested rules and guidelines of aggregation in cases where the identity of an individual or employer might likely be interpreted even though the rules and guidelines of aggregation have been followed.

2. All reports developed by the contractor shall only contain aggregated data. No disaggregate data identifying participants or employers shall be released to outside parties or to the public.

3. The data system of the contractor shall have prerelease edits, which shall not allow the production of data cells, which do not comply with the rules and guidelines of aggregation.

4. The guideline of a minimum data cell size for any combination of data shall be five participants.

APPENDIX B
CONTRACT EMPLOYEE:
CONFIDENTIALITY AGREEMENT

I (please print), _____, an employee of (please print) _____ _____ hereby acknowledge that the (Entity) records and documents are subject to strict confidentiality requirements imposed by state and federal law including (Site appropriate statutes here)

I (initial) _____ acknowledge that my supervisor, or the data librarian, has reviewed with me the appropriate provisions of both state and federal laws including the penalties for breaches of confidentiality.

I (initial) _____ acknowledge that my supervisor or the data librarian has reviewed with me the confidentiality and security policies of the (entity).

I (initial) _____ acknowledge that my supervisor or the data librarian has reviewed with me the policies of confidentiality and security of our organization.

I (initial) _____ acknowledge that unauthorized use, dissemination or distribution of CDSS confidential information is a crime.

I (initial)_____ hereby agree that I will not use, disseminate or otherwise distribute confidential records or said documents or information either on paper or by electronic means other than in the performance of the specific research I am conducting.

I (initial) _____ also agree that unauthorized use, dissemination or distribution is grounds for immediate termination of my organization's Contract/MOU with the (entity) and may subject me to penalties both civil and criminal.

_____ _____

Signed Date

GLOSSARY

Most terms in these guidelines are intended to be interpreted according to their generally accepted usage and meaning. The following terms have been defined to help add clarity to their usage in the Business Associate Agreement and related Appendices. Refer to the HIPAA legislation and related Rules for a complete list of definitions as promulgated in law.

Digital Certificate—a computer based record which:

1. identifies the certification authority issuing it;
2. names or identifies its subscriber;
3. contains the subscriber's public key; and
4. is digitally signed by the certification authority issuing or amending it, and
5. conforms to widely used industry standards, I cluding, but not limited to ISO x.509 and PGP certificate standards.

Digital Signature- digital signature is defined as an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.

Audit Trail--Systems information identifying source/location of access, date and time, user-id, targeted service and activity performed.

Contractor-- For the purposes of this document, the term "contractor' is used to describe an operating entity which contracts with a state agency or a research organization that enters into a Memorandum of Understanding (MOU) with the agency for access to Protected Health Information.

Information Assets—Information assets include anything used to process or store information, including (but not limited to) records, files, networks and databases; and information technology facilities, equipment (including personal computer systems), and software (owned or leased).

Information Security Incidents—Information Security incidents include, but are not limited to, the following: any event (intentional or unintentional) that causes the loss, damage to, destruction, or unauthorized disclosure of information assets. These incidents are classified in the following types: (1) viruses, (2) theft of CDSS information assets, (3) misuse of information assets, (4) destruction of information assets, (5) intrusions (electronic and physical), and (6) any other type of information security incident that does not fit into the previous categories.

Sensitive Data—Information maintained that requires special precautions to protect it from unauthorized modification or deletion. Sensitive information may be either public or confidential. Examples include statistical reports, financial reports and logon procedures.

BUSINESS ASSOCIATE AGREEMENT WORKGROUP PARTICIPANTS

Carr, Larry	Social Services	PhD., Research Program Specialist II
Sherman, Shneor	Health Services	Staff Information Systems Analyst
Self, Dennis	Mental Health	Program Specialist I
Styc, Kathy	Mental Health	Chief, Statistics and Data Analysis Branch
Jordan, Sherland	Social Services	Chief, Information Security and Management Systems Branch